## Schule Online –
## Lernen in der Digitalen Welt

# Hinweise zur sichereren Nutzung des Internets

Das Internet hat unsere Lebenswelt grundlegend verändert, nicht erst seit der Corona-Pandemie. Die Nutzung von E-Mail, Instant-Messengern, Videokonferenzsystemen, Online-Banking usw. sind im privaten und beruflichen Kontext alltäglich geworden. Wir verlagern einen immer größeren Teil unserer Aktivitäten in die digitale Welt.

(Personenbezogene) Daten werden häufig als die „Währung des 21. Jahrhunderts" bezeichnet. Leider lässt sich im Internet nicht nur mit legalen Mitteln viel Geld verdienen. Kriminelle haben es auf diese Währung abgesehen und versuchen Kapital aus der Unwissenheit und Unachtsamkeit von Menschen zu schlagen. Diese Handreichung* soll dabei helfen, Sicherheitsrisiken durch einfache, auch für IT-Laien praktikable Maßnahmen zu minimieren. Durch die Umsetzung der verlinkten Handlungsempfehlungen wird das Risiko reduziert, Opfer von Internetkriminalität zu werden:

- Empfehlung 1: Sichere Kennwörter nutzen
- Empfehlung 2: Nutzung von Virenscanner & Firewall
- Empfehlung 3: Ignorieren von verdächtigen E-Mail-Anhängen
- Empfehlung 4: Downloads aus sicheren Quellen
- Empfehlung 5: Regelmäßige Sicherung durch Backups
- Empfehlung 6: Verwendung von Sicherheitsfunktionen des Browsers
- Empfehlung 7: Anlegen unterschiedlicher Benutzerkonten
- Empfehlung 8: Sicherung des WLAN
- Empfehlung 9: Verwaltung von Cookies
- Empfehlung 10: Updates sollten stets durchgeführt werden

*Damit dieses Angebot den Bedürfnissen möglichst vieler Nutzerinnen und Nutzern entspricht, wird an dieser Stelle auf konkrete Empfehlungen zu Produkten und/oder Websites verzichtet. Zusätzlich würden die Angaben zu den Produkten durch die fortlaufende Weiterentwicklung ihre Gültigkeit verlieren.

# Schule Online –
# Lernen in der Digitalen Welt

## Empfehlung 1: Sichere Kennwörter nutzen

Für jedes Online- und Benutzerkonto sollte **ein eigenes** Kennwort genutzt werden! Dieses Kennwort sollte

- mindestens aus 10 Zeichen,
- sowie aus Groß- und Kleinbuchstaben,
- als auch aus Zahlen und Sonderzeichen bestehen.

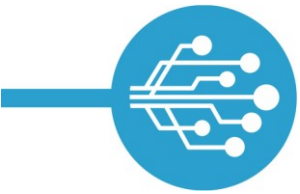
Einfache Wörter, die in Wörterbüchern stehen und leicht mit dem Nutzer oder der Nutzerin in Verbindung gebracht werden können (eigenes Geburtsdatum…) oder die gängige Zeichenfolgen oder Tastaturmuster beinhalten (qwertz; 23456…) sollten *nicht* verwendet werden. Und auch ein neu zu vergebenes Kennwort darf nicht wie das alte Kennwort lauten.

Eine Idee wäre, von einem Satz immer nur die Anfangsbuchstaben zu nehmen: Ich denke oft an meine 2 Lieblingstiere, die Katzen Max und Paule. Das Kennwort wäre dann: Idoam2L,dKMuP

Da es dadurch in der Praxis sehr schwer fallen kann, sich alle nach diesen Regeln erstellten Passwörter zu merken, empfiehlt sich die Verwendung eines Password-Managers. Diese Programme speichern Anmeldedaten verschlüsselt entweder in der Cloud oder auf einem Speichermedium. Statt vieler unterschiedlicher Kennwörter muss dann nur noch ein Master-Password gemerkt werden. Dieses sollte natürlich hinreichend komplex gewählt werden, idealerweise richtet man zusätzlich ein zweites Authentifizierungsverfahren ein. Denn *erlangt eine unbefugte Person Zugriff auf den Password-Manager, sind alle Kennwörter verloren!*

## Empfehlung 2: Nutzung von Virenscanner & Firewall

Virenscanner schützen das Endgerät vor Schadsoftware. Sie erkennen, blockieren und beseitigen viele Gefahren automatisch, ersetzen jedoch keinesfalls die anderen Maßnahmen. In den gängigen Betriebssystemen sind Virenscanner bereits enthalten. Diese reichen aus und haben den Vorteil, dass keine zusätzliche Software installiert werden muss, die ggf. selbst ein Sicherheitsrisiko darstellen kann. Zudem sind sie optimal an das Betriebssystem angepasst und beeinträchtigen die Performanz des Rechners vergleichsweise wenig. Wichtig: Virenscanner können nur bereits bekannte Schadsoftware bekämpfen. Daher muss gerade dieses Programm immer auf dem neuesten Stand sein. Die Option „automatische Updates" sollte daher aktiviert sein.





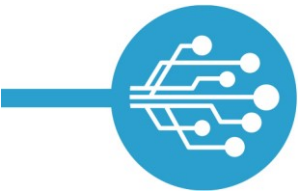
Firewalls sind in den gängigen Betriebssystemen ebenfalls integriert. Sie sollten unbedingt aktiviert sein, damit der Rechner gegen unerwünschte Netzwerkzugriffe geschützt wird.

## Empfehlung 3: Ignorieren von verdächtigen E-Mail-Anhängen

Unerwünschte und massenhaft versendete E-Mails werden als **Spam- oder Junk-Mails** bezeichnet. Auch wenn die Spamfilter der E-Mail-Provider einen Großteil dieser lästigen Mails blockieren, gelingt dies niemals vollständig. Nutzerinnen und Nutzer können unerwünschte Mails als Spam markieren und so mithelfen, die Blockiermechanismen zu verbessern. Außerdem sollte im Mailprogramm das Laden weiterer Inhalte standardmäßig deaktiviert sein: Die Versender von Spam-Mails nutzen diese Funktion nämlich, um herauszufinden, ob Mailadressen aktiv sind.

Ziel von sogenannten **Phishing-E-Mails** ist es, an die persönlichen Daten, z. B. Kennwörter von Nutzerinnen und Nutzern, zu gelangen. Dafür versenden Kriminelle E-Mails, die vorgeben von einem Geldinstitut, einer Regierungsbehörde, einem bekannten und vertrauenswürdigen Unternehmen oder anderen als seriös erscheinenden Kommunikationspartnern zu stammen. Häufig enthalten diese E-Mails gefährliche Links oder Dateianhänge oder die Aufforderung, persönliche Daten einzugeben. Phishing-Mails sollten sofort gelöscht werden, damit man sie nicht versehentlich doch noch öffnet. Als allgemeine Regel gilt: Banken, Behörden etc. werden *niemals* Nutzerdaten per Mail von Ihnen verlangen! Im Zweifel sollte über einen anderen Kommunikationsweg (z. B. Anruf) mit dem vermeintlichen Absender Kontakt aufgenommen werden.

Besondere Vorsicht ist bei **Mail-Anhängen** geboten. Das gilt nicht nur für Dateien, die von vorneherein als Software zu erkennen ist. Bereits die mit gängiger Bürosoftware erstellten Texte, Tabellen etc. können gefährliche Bestandteile enthalten. Bestehen Zweifel an der Authentizität des Versenders (etwa, wenn ein Anhang nicht erwartet wird), sollten Anhänge *nicht* geöffnet werden. Im Zweifel sollte beim Versender nachgefragt werden.



## Schule Online –
## Lernen in der Digitalen Welt

### Empfehlung 4: Downloads aus sicheren Quellen

(Kostenlose) Software-Downloads werden im Internet in großem Umfang angeboten. Beim Download können jedoch auch zusätzliche, potenziell gefährliche Programme mit heruntergeladen werden, ohne dass die Nutzerin oder der Nutzer dies erfährt und ohne, dass Virenschutzprogramme dies in jedem Fall anzeigen. Kostenfreie Software sollte daher grundsätzlich direkt beim Hersteller bezogen werden.

### Empfehlung 5: Regelmäßige Sicherung durch Backups

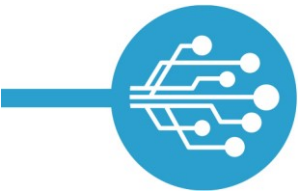
Der Zugriff auf die eigenen Daten kann aus verschiedenen Gründen unmöglich werden, beispielsweise durch einen Festplatten-Defekt oder den Angriff mit sogenannter Ransomware (Schadsoftware, die Daten durch Verschlüsselung für die Eigentümerin oder den Eigentümer unzugänglich macht).

In solchen Fällen ist die Wiederherstellung des Zugriffs schwierig bis unmöglich, in den meisten Fällen sind die Daten verloren. Daher sollte regelmäßig eine Kopie aller relevanten Daten auf einem externen Speichermedium oder in einer Cloud angefertigt werden (sofern ein externes Medium verwendet wird, sollte dies an einem anderen Ort als die Daten-Quelle aufbewahrt werden!). Da dies händisch in den meisten Fällen nicht praktikabel ist, sollte eine entsprechende Backup-Software verwendet werden, welche Quelle und Backup vergleicht und nur Änderungen überträgt. Wichtig ist es, Backups als *regelmäßige* Routine einzurichten, damit Datenverluste minimiert werden. Sowohl die Quelldaten als auch die Backups sollten *immer* verschlüsselt werden, damit Unbefugte keinen Zugriff haben. Verschlüsselungsprogramme sind in den gängigen Betriebssystemen bereits integriert, müssen aber aktiv eingerichtet werden. Selbstverständlich sollten auch hier sichere Kennwörter gewählt werden.

### Empfehlung 6: Verwendung der Sicherheitsfunktion des Browsers

**Lesezeichen**: Für den Aufruf häufig besuchter Internetanwendungen wie beispielsweise LOGINEO NRW, das Online-Banking oder das favorisierte Nachrichtenportal ist das Setzen von Lesezeichen im Browser sinnvoll. Das ist nicht nur bequem, sondern minimiert auch das Risiko, dass man beispielsweise durch Buchstabendreher oder betrügerische Links auf Internetseiten mit Schadsoftware weitergeleitet wird.

**Passwortmanager**: Die meisten Browser bieten an, Zugangsdaten auf Webseiten zu speichern und automatisch einzutragen. Diese Funktion ist kritisch zu bewerten: Einerseits ist das Feature praktisch, da es im



## Schule Online –
## Lernen in der Digitalen Welt

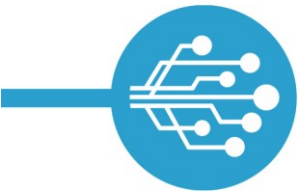
Arbeitsalltag das ständige Eingeben von Passwörtern erspart, andererseits stehen die gespeicherten Passwörter anderen Personen zur Verfügung, sofern diese Zugang zu dem Browser haben. In vielen Fällen können sie auch ausgelesen werden. Besser ist es, einen separaten Password-Manager (siehe Kennwörter) zu verwenden, der als verschlüsselte Datei in der Cloud oder auf einem (mobilen) Speichermedium zur Verfügung steht.

**Internet-Verbindungen**: Grundsätzlich sollte sparsam mit der Übermittlung eigener Daten im Internet umgegangen werden. Besonders beim Online-Shopping, Online-Banking oder bei Anmeldungen sollte geprüft werden, ob Daten verschlüsselt übertragen werden.
Ein Hinweis für eine gesicherte Internetverbindung ist das Präfix **https://** vor einer URL. Dies zeigt an, dass eine Datenverschlüsselung zwischen dem eigenen Endgerät (Client) und dem Server, auf dem die Internetseite gehostet wird, besteht.
Viele Browser überprüfen die für eine sichere Datenübertragung notwendigen Sicherheitszertifikate von Webseiten und zeigen den Nutzerinnen und Nutzern durch das Symbol eines geschlossenen Vorhängeschlosses in der Browseradresszeile sichere Verbindungen an.

**Überprüfen der Link-URL**: Bevor man einem zugesandten Link folgt, kann der hinterlegte Linktext überprüft werden. Bei einer im Text verlinkten Datei lässt sich der Link durch das sogenannte Mouseover (Herüberbewegen der Maus bzw. des Cursors über das als Link gekennzeichnete Wort) anzeigen. Fallen dabei verdächtige Begriffe auf, sollte der Link nicht angeklickt werden. Alternativ kann der Link im Browserfenster angezeigt werden.

## Empfehlung 7: Anlegen unterschiedlicher Benutzerkonten

Arbeiten verschiedene Nutzerinnen und Nutzer an einem Computer, so ist das Einrichten von unterschiedlichen Benutzerkonten sinnvoll.
Jedes Benutzerkonto kann dann nicht nur den persönlichen Vorlieben entsprechend angepasst, sondern auch sicher verwaltet werden. Dateien, die ein Nutzer oder eine Nutzerin abgelegt hat, liegen in einem Verzeichnis, auf das niemand sonst Zugriff hat. Zudem haben normale Nutzerkonten im Vergleich zu Administratorenkonten eingeschränkte Rechte – das ist ein Vorteil, wenn beispielsweise doch Schadsoftware auf den Rechner gelangt ist.



# Schule Online – Lernen in der Digitalen Welt

## Empfehlung 8: Sicherung des WLAN

Das heimische WLAN sollte unbedingt im aktuellen Standard WPA2 verschlüsselt sein, da im Falle eines unbefugten Zugriffs neben dem Netzwerk selbst auch Daten zugänglich sind. Grundsätzlich sollte der bei der Einrichtung voreingestellte Netzwerkname und der Netzwerkschlüssel geändert werden, damit Hacker keine Informationen über den Router erhalten. Auch für den Netzwerkschlüssel gelten die Ansprüche an sichere Kennwörter.
WLAN-Router sind selbst kleine Computer mit eigenem Betriebssystem. Diese Firmware muss unbedingt auf dem neuesten Stand gehalten werden, am besten durch automatische Updates.
Wenn möglich kann auch das WPS (Abkürzung für *Wi-Fi Protected Setup*), das normalerweise einen schnellen Verbindungsaufbau von WLAN-Geräten wie WLAN-Druckern unterstützt, deaktiviert werden. Neue Geräte müssen dann über einen manuellen Verbindungsaufbau in das WLAN eingebunden werden.

## Empfehlung 9: Verwaltung von Cookies

Cookies sind kleine Textdateien, die beim Aufrufen von Webseiten erstellt und auf dem Rechner des Nutzenden gespeichert werden. Sie sind teilweise notwendig, damit die Seite funktioniert, teilweise werden darüber aber auch Daten gesammelt, die die Nutzerin bzw. den Nutzer identifizierbar machen und beispielsweise für Werbezwecke verwendet werden können.
Webseiten fragen in aller Regel ab, welche Cookies zugelassen werden sollen – hier sollte der oft unbequeme Weg individueller Einstellungen gegangen und alle nicht notwendigen Cookies abgelehnt werden. Zusätzlich sollten im Browser die Einstellungen so vorgenommen werden, dass Drittanbietercookies standardmäßig abgelehnt werden. Werden Cookies automatisch beim Schließen des Browsers gelöscht, gibt man weniger Daten preis, muss aber ggf. mit Unbequemlichkeiten leben, weil man beispielsweise bei einem späteren Besuch von Webseiten Eingaben wiederholen muss.

## Empfehlung 10: Updates sollten stets durchgeführt werden

Die Hersteller von Computer-Software schließen bekannt gewordene Sicherheitslücken in ihren Produkten. Daher ist es wichtig, die Software (vor allem Betriebssystem, Virenschutzprogramm, Internetbrowser und Router) durch die Aktivierung automatischer Updates auf dem aktuellen Stand zu halten.

# Schule Online –
# Lernen in der Digitalen Welt

## Glossar

- Browser: Programm bzw. App, mit der Internetseiten angezeigt werden können.
- Cookie: Textdatei, die während des Besuchs einer Webseite auf einem Computer platziert wird und verschiedene Informationen über Nutzer und Nutzerinnen sammelt.
- Malware: engl. für Schadsoftware (Virus / Trojaner / Spähprogramme)
- Phishing-E-Mail: Kunstwort aus *Passwort* und *fishing*. E-Mails, die Anhänge oder Links enthalten und versuchen, sensible Daten von Nutzerinnen und Nutzern abzugreifen.
- Ransomware: engl. für Erpressungssoftware. Damit wird das Betriebssystem als „Geisel" genommen, es befindet sich unter der Kontrolle der Betrüger. Man wird aufgefordert zur Freigabe ein Lösegeld zu zahlen.
- Spam- / Junk-E-Mail: Bezeichnung für unerwünschte und massenhaft zugestellte E-Mails, die meistens Werbung enthalten.
- Trojaner: auf den ersten Blick ein nützliches Programm, das sich später als Schadprogramm (s.o.) erweist.
- Virus: eine Form von Schadsoftware.
- WPA2: *Wi-Fi Protected Access 2,* Weiterentwicklung des WPA-Standards, auf einem Funkstandard basierende Verschlüsselungsmethode. Modernster WLAN-Sicherheitsstandard.

Herausgeber: Medienberatung NRW